Guidelines for Sensitive Computer Systems

Introduction

This document is intended to give some practical guidance in determining when computer based information should be considered sensitive and additional protective measures need to be applied to the systems used to process that information. This is not a comprehensive or authoritative description of sensitive information. For that information, see the Department of Energy's (DOE) Sensitive Subjects List (SSL) at https://www.ameslab.gov/files/doe_sensitive_subjects_list.pdf and Guide 10200.007, Guide to Identifying and Protecting Official Use Only (OUO) Information. This document only contains selected subjects that have been known to cause uncertainty.

Questions regarding Sensitive or Export Control information can be directed to Deb Covey, Export Control Manager, 4-1048.

Topics on the Sensitive Subjects List

- **Topics related to Nuclear Weapons and Nuclear Fuel Cycle;**
- **Topics related to rockets, missiles, and delivery systems;**
- **Topics related to conventional arms and other defense-related technologies;**
- **Topics related to Chemical and Biological weapons;**
- **Topics Related to Advanced Scientific Computers and Software;**

  This information only includes high-performance computing technology **that meets or exceeds the Million Theoretical Operations per second (MTOP) limit specified for Tier 3 countries in section 742.12 of the Export Administration Regulations (EAR);** in other words, *normally* those with more than 190,000 MTOPs.

  In addition proprietary software, or source code developed for systems meeting the MTOP limit specified above, is considered sensitive data.

- **Topics Related to Business Sensitive (Proprietary) Information.**

  Information is business sensitive or proprietary when it falls into one of the following situations:

  1. It is data related to a CRADA or work-for-others (WFO) project **and the sponsor(s) in the project have indicated that this data is protected CRADA data or proprietary information.**
  2. It is data that involves technology that will be patented and a patent application has **not yet been filed, or is covered in a Non-Disclosure Agreement (NDA).**
  3. Export controlled information identified by the Department of Commerce (DOC).
  4. Information intended for use in crime control or criminal investigations, including information that a Law Enforcement Agency has requested remain unpublished.
  5. Research that cannot be published for other reasons related to restricting public knowledge.

Personal Information

This information includes private information about individual employees of Ames Laboratory; i.e. anything not found in the phone book or through legal Internet searching, such as Social Security numbers or medical information.

Moderate Computer Systems

A computer system should be considered sensitive and additional protections should be applied **only if the sensitive data is stored on the computer system.** These devices are considered 'moderate computer systems'. For instance, if a spreadsheet containing social security numbers is saved on the 'C' drive, then the system should be considered moderate. If that same spreadsheet is saved on another server (i.e. alto.ameslab.gov, a moderate data storage server), and is opened remotely from the local machine, then only the server needs to be considered moderate.

Some ways in which the burden of sensitive information can be eased are:

- Utilize central systems that are already labeled moderate, for example the central data storage server, or the central personnel database;
- Consolidate sensitive information storage to as few machines as possible.

For details on the computer security rules for working with all systems, see the Rules of Behavior https://www.ameslab.gov/files/forms/form_48400.019_rev4.1.pdf.

The following is a summary of the different controls that need to be applied to sensitive information on computer systems:

- The storage location of sensitive information must be on a designated, approved moderate computer system: a system used solely for this project, and only accessible by administrators and researchers working on the project.
- User accounts on moderate computer systems must be administered by the Information Systems office. Accounts idle for more than 90 days must be disabled.
- Administrative access to moderate computer systems is uses two-factor authentication (Cryptocards).
- Moderate computer systems must be stored in areas which are either staffed or locked at all times.
- Sensitive data may not be recorded on personal computer media (ie CD-ROMs, usb keys).
- Sensitive data should be backed up on a regular basis. Backups must be encrypted, and backup media destroyed physically when it is expired.
- Electronic transmission of sensitive data outside of the Laboratory must use encryption.
- Programs and files utilizing private personnel information or proprietary information may be accessed only on Ames Laboratory computer resources.
- Workstations used to access sensitive data must have 10 minute screensaver locks enabled.
- Visitors must be logged in an access log.
- Moderate computer systems need to send logs to the central logging server, and apply host-based intrusion detection software to monitor system changes.